Attorney Docket No.: 16869P-078100US
Client Reference No.: 340200560US1

PATENT APPLICATION

CONTROL METHOD FOR INFORMATION NETWORK SYSTEM, INFORMATION NETWORK SYSTEM AND MOBILE COMMUNICATION TERMINAL

Inventor: Yoshihisa Makuta, a citizen of Japan, residing at
New Marunouchi Bldg., 5-1
Marunouchi 1-Chome
Chiyoda-ku
Tokyo, 100-8220 Japan

Assignee: HITACHI, LTD.
New Marunouchi Building, 5-1
Marunouchi 1-chome
Chiyoda-ku
Tokyo, 100-8220 Japan

Entity: Large

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 650-326-2400

CONTROL METHOD FOR INFORMATION NETWORK SYSTEM, INFORMATION NETWORK SYSTEM AND MOBILE COMMUNICATION TERMINAL

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application relates to and claims priority from Japanese Patent Application No. 2002-205072, filed on July 15, 2002, the entire disclosure of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of The Invention

[0002] The present invention relates to an information network technology and a mobile communication terminal, and more particularly to an authentication technology for an authentication server performing shared control of a file based on the position information of each terminal and file server, in an environment where a plurality of terminals and file servers which have a sharable information resource, such as a file, are connected to be a network via cable or radio transmission.

Description of the Related Art

[0003] Terminals and file servers are connected via a network to share information. In a radio network connection, the terminals and file servers can establish communication via access points of a radio LAN using radio waves.

[0004] However, the radio waves reaching range is undefined, so it is possible that an unexpected terminal which exists in the radio waves reaching range connects to the network, and a user with ill intent may operate the terminal and obtain information from another terminal or file server without leaving any evidence of their presence.

[0005] In the above mentioned prior art, where the range in which the radio communication is possible is not restricted, the case when an unexpected or unauthorized terminal which exists in the radio waves reaching range is connected to the network is not considered, and a leak of information may occur, which has been a technical problem.

[0006] Japanese Patent Laid-Open No. 2000-215169 discloses a technology where a specified data set is assigned for each access point to the LAN of the radio terminal, so that the specified data set is accessed automatically each time an access point changes, but the position information used for identifying the position of this radio terminal is only the position information of the access point. Therefore it is possible, for example, that an access point is assigned to each room of a building and an accessible data set can be switched each time the user moves out of each room, but access from outside the building cannot be identified, where the above mentioned technical problem, such as information leakage, is still unresolved.

SUMMARY OF THE INVENTION

[0007] The present invention is directed to a control method for an information network system which is comprised of a cable or radio information network and a plurality of information processing units connected thereto, wherein accessibility to an information resource on the information network of the information processing unit is controlled using the first position information on the connection position of each one of the information processing units with respect to the information network and the second position information to indicate the current position of the information processing unit.

[0008] More specifically, for example, the current position information (second position information) of the terminal and file server which are network-connected via cable or radio is obtained, the respective communicable range is set at the authentication server based on the respective current position information of the terminal and file server and position information (first position information) of the access point (network segment), and information is transmitted/received from/to a terminal and server in the restricted range respectively.

[0009] In the above configuration, the position information of the terminal and file server is obtained based on the information determined from the distance between the terminal or file server itself and a plurality of GPS satellites. Alternatively, the position information of the terminal and file server is obtained based on the information obtained from the distance between the terminal or file server itself and a plurality of portable telephone base stations. In other embodiments, the position information of the terminal and file server is obtained

based on the position information of the terminal or file server itself and the radio LAN access point to which the terminal and file server can be connected.

[0010] In the above configuration, the authentication server decides the communicable range of each terminal and file server, and controls the communication range using the position information received from each terminal and file server.

[0011] The terminal or file server can fetch a file from another terminal or file server via the authentication server.

[0012] When an access request to a terminal is out of the communicable range of a terminal, the authentication server performs access control not to approve access to the terminal.

[0013] It is a feature of the present invention to restrict the range in which communication is possible so that network connection from an unexpected terminal is rejected, and to provide a network connection environment only in a restricted range so that accurate information transfer, free from information leakage and a disguised user, is enabled.

[0014] It is another feature of the present invention for each terminal and file server to obtain respective position information from the distance between each terminal or file server and a plurality of GPS satellites or a plurality of portable telephone base stations.

[0015] It is still another feature of the present invention to determine the communicable range of each terminal and file server, and control the communication range at an authentication server using the position information received from each terminal and file server.

[0016] In one embodiment, a method of providing access to an information unit by a wireless unit comprises providing a first position information containing an access enabled area for the wireless unit, wherein the access enabled area falls within a range of communicable area of a wireless access point; and obtaining a second position information containing a current position of the wireless unit. If the current position of the wireless unit is within the access enabled area for the wireless unit, access if permitting to the information unit by the wireless unit. If the current position of the wireless unit is outside the access enabled area for the wireless unit, access to the information unit is denied by the wireless unit even if the current position of the wireless unit is within the range of communicable area of the access point.

[0017] In another embodiment, a system for providing access to an information unit by a wireless unit comprises a memory including a first position information containing an access enabled area for the wireless unit, wherein the access enabled area falls within a range of communicable area of a wireless access point. A position module is configured to obtain a second position information containing a current position of the wireless unit. An access module is configured, if the current position of the wireless unit is within the access enabled area for the wireless unit, to permit access to the information unit by the wireless unit, and, if the current position of the wireless unit is outside the access enabled area for the wireless unit, to deny access to the information unit by the wireless unit even if the current position of the wireless unit is within the range of communicable area of the access point.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Fig. 1 is a simplified schematic diagram depicting an example of the configuration of the information network system for embodying the control method for the information network system according to an embodiment of the present invention;

[0019] Fig. 2 is a simplified schematic diagram depicting an example of the information table which is used in the control method for the information network system according to an embodiment of the present invention;

[0020] Fig. 3 is a simplified schematic diagram depicting a variant form of the configuration of the information network system for embodying the control method for the information network system according to an embodiment of the present invention;

[0021] Fig. 4 is a simplified schematic diagram depicting an application example of the information network system for embodying the control method for the information network system according to an embodiment of the present invention;

[0022] Fig. 5 is a flow chart depicting an example of the operation of the file server in the information network system according to an embodiment of the present invention;

[0023] Fig. 6 is a flow chart depicting an example of the operation of the authentication server in the information network system according to an embodiment of the present invention; and

[0024] Fig. 7 is a flow chart depicting an example of the operation of the terminal in the information network system according to an embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0025] Embodiments of the present invention will now be described in detail with reference to the accompanying drawings.

[0026] Fig. 1 is a simplified schematic diagram depicting an example of the configuration of the information network for embodying the control method for the information network system according to an embodiment of the present invention.

[0027] In the present embodiment, the information network will be described using a network system where each terminal obtains position information by GPS (Global Positioning System) respectively and decides which terminals are shared at the authentication server as an example.

[0028] As Fig. 1 shows, the network system of the present embodiment is comprised of a plurality of wireless units or terminals 300, 301, 311 – 315 (hereafter generalized as terminal 3xx) each of which has a sharable file and can freely move, file servers 411 – 413 (hereafter generalized as 41x) each of which has a sharable file and is fixed at a specified position, authentication server 400 which collects position information of the terminal 3xx, decides the accessible range of each terminal and controls access, radio LAN access point 101 which is installed for connecting each terminal 3xx to the authentication server 400, and a plurality of GPS satellites 501, 502, 503 (hereafter generalized as 50x) which are used for obtaining position information of the terminal 3xx.

[0029] Each one of the terminals 3xx has a radio LAN access function 300a for performing radio communication with the radio LAN access point, GPS reception function 300b for obtaining current position information of the terminal 3xx in communication with the GPS satellite 50x, and a function to send this current position information to the radio LAN. Each one of the file servers 41x can also have a function to obtain position information of itself and send it to the authentication server 400.

[0030] The authentication server 400 includes a memory 400a which stores a first position information containing an access enabled area for a terminal, a position module 400b which receives from the terminal a second position information containing the current position of

the terminal, and an access module 400c which controls access to the information units such as file servers by the terminal according to the method described herein below.

[0031] When the terminal 3xx includes a portable telephone function, a function to obtain the current position from the positional relationship with the base station, which is not illustrated, in a public portable telephone network, is installed as the GPS reception function 300b.

[0032] Fig. 2 is a simplified schematic diagram depicting an example of a configuration of the information table to be used for authentication processing for controlling the approval of access of a terminal or a file server which has a sharable file to a terminal depending on the area.

[0033] In the information table 600 of the present embodiment, access enabled area 600b, reception enabled range 600c represented by the enabled range (x, y) coordinates, access destination terminal list 600d, and access origination terminal list 600e are stored and associated with each one of the radio LAN access points 600a. The reference characters of the radio LAN access point 600a, access enabled area 600b, access destination terminal list 600d, and access origination terminal list 600e correspond to the reference characters of the various elements and components in Fig. 1.

[0034] For the numeric values of the enabled range (x, y) coordinates of the reception enabled range 600c, simple numeric values are set to simplify the description; however in reality the reference values of authentication based on the current position (longitude, latitude, etc.) of each terminal, for example, are set.

[0035] Referring to the example in the first row 601 of the information table 600, the file server 411, which has a sharable file, wherein an area 211 is set as an accessible area, is stored in the information table 600. The terminal 311 in the area 211 can communicate with the radio LAN access point 101, and can obtain information from the GPS satellite 50x. The terminal 311 obtains information from the GPS satellite 50x and calculates the position information of the terminal 311 itself based on that information. The terminal 311 transmits the position information of itself to the authentication server 400 via the radio LAN access point 101. The terminal 311 immediately replies with the current position information of itself when transmission of position information for itself is requested from the authentication server 400.

[0036] As a current position information transmission method for this terminal, it is possible to use a vender unique area in the information frame when connection of a standard radio LAN protocol is started. When position information is set in a predetermined format in this vender unique area, the authentication server executes the later mentioned authentication processing, such as enabling access to a file server, regarding that the terminal at the transmission source has a function corresponding to the authentication technology according to the present embodiment. When the position information is not set, the terminal can execute such processing as accessing only general public data with the lowest security level as a general terminal. By this, the authentication functions of the present embodiment can be implemented without damaging the universality of the currently used radio LAN protocol.

[0037] The flow chart in Fig. 7 shows an example of operation of such a terminal 3xx. At first, operation for obtaining the current position information of the terminal 3xx itself from GPS (step 921) is repeated until the current position enters the communicable area of the nearest radio LAN access point (step 922), and when the current position enters the communicable area, the terminal 3xx transmits, to the authentication server 400, the current position information of the terminal 3xx and position information of the currently connected radio LAN access point (network segment) via the radio LAN access point to request access (step 923). The terminal 3xx then waits for the access enable signal (step 924) and, if access is enabled (step 925), access is requested to the file server (step 926) and data is obtained (step 927). If access is disabled, access to the file server is not executed (step 928).

[0038] When the position information of the received terminal 311 is within the access enabled range of the information table 600 in Fig. 2, the authentication server 400 adds the terminal 311 to the access origination terminal list 600e.

[0039] To the terminal registered in the access origination terminal list 600e, the terminal 311 requests the position information of that terminal at a constant interval, and if the position information of the received terminal is outside the access enabled range of the information table 600, or if no replay to the position information is received, the terminal information is deleted from the access origination terminal list 600e.

[0040] When the terminal 311 attempts to obtain information from the file server, the terminal 311 inquires the authentication server 400 about the terminals which are allowed access to the area 211 where the terminal 311 is positioned.

[0041] Referring to the information table 600, where information of the terminal 311 is in the access origination terminal list 600e indicated by the row 601 corresponding to the area 211, the authentication server 400 allows the terminal 311 to access the file server 411 which is registered in the access origination terminal list 600d corresponding to the area 211. As a result of referring to the information table 600, if the information on the terminal 311 does not exist in the access origination terminals indicated by the row 601 corresponding to the area 211, the access is not approved, regarding that the terminal 311 is already outside the area 211. By this, the terminal 311 can obtain information from the file server 411 via the radio LAN access point 101 and the network as long as the terminal 311 is in the area 211.

[0042] The same procedure can be used for other terminals. As shown in Fig. 2, the terminal 312 in the area 212 can access the file server 412. The terminals 313 and 314 in the area 213 can access the file server 413 and the terminal 300. The terminal 315 in the area 214, which is connected to the network via another radio LAN access point 102, is in range to access the terminal 312 and the terminal 301, but can access only the terminal 312, since the terminal 301 is not connected to the network.

[0043] The terminal 301 in the area 200, which cannot communicate with any radio LAN access point, cannot connect to the authentication server 400. When the terminal 301 enters the communication enabled range of the radio LAN access point 101 or 102, then the terminal 301 succeeds in connection to the authentication server, and can communicate according to the access setting of the area.

[0044] An example of operation of the above mentioned authentication server will now be described with reference to the flow chart in Fig. 6.

[0045] The authentication server monitors whether an arbitrary terminal 3xx is in the communicable range of an arbitrary radio LAN access point (step 911), and if it is in the communicable range, the authentication server obtains the current position information of this terminal from this terminal (step 912), checks whether the current position of this terminal is within the reception enabled range which is set for each radio LAN access point (step 913), and if it is within the reception enabled range, the authentication server transmits the access enabled signal to this terminal (step 914), and adds this terminal to the access origination terminal list of the information table 600 (step 915). If the terminal 3xx is outside the range in step 913, the authentication server notifies access disabled to this terminal (step 916) and deletes this terminal from the access origination terminal list (step 917).

[0046] An example of operation of the file server will now be described with reference to Fig. 5. The file server monitors the access request from an arbitrary terminal (step 901), and if access is not requested, transmission/reception with this terminal is stopped (step 902). If access is requested, the file server judges whether the terminal is supported with such an information distribution service as the multimedia information of this file server (step 903), and if the terminal is not supported, the file server notifies the service guide (step 904). If the terminal is supported with the service, the file server checks whether this terminal is registered in the access origination terminal list (step 905), and if it is registered (that is, authenticated), the file server establishes transmission/reception with this terminal (step 907). If this terminal is not registered, the file server sends an access disabled message to this terminal (step 906).

[0047] If the radio LAN access points 101 and 102 have areas which cover different floors in the same building, the authentication server 400 cannot know which floor where the terminal exists merely by the position information obtained from the GPS satellite. To solve this technical problem, the present embodiment records the radio LAN access point (network segment) used by the terminal (first position information) as well in advance, and uses this information for authentication along with the current position of the terminal (second position information), so the difference in height direction can be considered. This uses the fact that radio waves used for a radio LAN do not pass through the walls of buildings.

[0048] As Fig. 3 shows, the radio LAN access points 101 and 102 are installed on the first floor 211a (1F) and second floor 214a (2F) of the two storey building 700 respectively, the area 211 is set to the floor range of the first floor 211a as the access enabled area of the terminal to the radio LAN access point 101, and in the same way, the area 214 is set to the floor range of the second floor 214a as the access enabled area of the terminal to the radio LAN access point 102. And the authentication server 400 uses the position information of the radio LAN access points 101 and 102, in addition to the current position information of individual terminals 311 and 315, for authentication to decide accessibility to data of the file server 41x, so that individual terminals 311 and 315 positioned on each floor can be identified accurately, and appropriate data access control becomes possible.

[0049] The advantage of this method is that communication for sharing a file with a terminal outside the specified range can be blocked even if the terminal is within the range of communicable areas 201 and 202 of the radio LAN access points 101 and 102, and it is

unnecessary to provide the terminal side with a special mechanism for this system. Therefore this system can be used for eliminating invalid terminals.

[0050] In other words, even if the radio waves of the radio LAN leaks from the building 700, and a terminal positioned outside the building 700 can connect to the radio LAN, the current position information of the terminal is judged to be outside the access enabled area, so authentication fails and the security of data access can be maintained.

[0051] By applying the authentication method of the above mentioned embodiment, this system can be applied to operating the CD shop shown in Fig. 4, for example. In the CD shop 800, an area is decided for each music category, where the area 21 is an area where rock CDs are displayed, and the area 22 is an area where jazz CDs are displayed. The music file for trial listening, corresponding to each area, is stored in the file server 41. The area 21 and area 22 correspond to rock music and jazz music trial listening data respectively by the authentication server 40.

[0052] If a customer, who has a portable telephone 3 comprised of the radio LAN access function 3a to the radio LAN access point 1 which includes the CD shop in the communicable range 20 and GPS reception function 3b from the GPS satellite 50x, is walking in the CD shop and attempts to listen to music data operating the portable telephone 3 in the area 21, the authentication server 40 sends the rock music trial listening data to the portable telephone 3 based on the current position information of the portable telephone 3, and by this, the rock music trial listening data is displayed on the screen of the portable telephone 3, and the data can be listened to. In the same way, if the portable telephone 3 leaves the area and enters the area 22, rock music cannot be listened to, but instead jazz music can.

[0053] If the area 21 and area 22 are on different floors of the same building, similar switching and authentication can be performed by using the position information of the radio LAN access point as well, as mentioned above. By using this method, the trial listening data can be provided only to the portable telephone 3 located in a specified range, and invalid use of trial listening data from outside the range can be prevented.

[0054] Various other application methods are possible, such as ways of preventing a leak of in-house information to outside an office.

[0055] As described above, according to the present embodiment, in an environment where a plurality of terminals 3xx and file servers 41x, which have a sharable file are network-connected via cable or radio, the authentication server 400 controls the sharing of the file based on the position information of each terminal and file server 41x, so access control to the file on the network becomes possible, which is effective to prevent invalid access, and access from a disguised user.

[0056] In each terminal 3xx and file server 41x, the position information of each terminal or file server itself is obtained from the distance between the terminal or file server itself and a plurality of GPS satellites 50x or a plurality of portable telephone base stations, and for this, only a GPS receiver or portable telephone receiver is installed to the terminal 3xx and file server 41x, and GPS satellites or portable telephone base stations have already been organized, so without adding a major investment to the current equipment, invalid access and access from a disguised user can be effectively prevented.

[0057] Also the authentication server 400 decides the communication possible range of each terminal and file server and controls the communication range, from the position information received from each terminal 3xx and file server 41x, so communication is enabled only for access based on correct position information, so invalid access and access from a disguised user can be effectively prevented.

[0058] The present invention provides a file access authentication method characterized in that in an environment where a plurality of terminals and file servers, which have sharable files, are network-connected via cable or radio, an authentication server controls the sharing of the file based on the position information of the respective terminal and file server. In some embodiments, the position information of the terminal or file server itself is obtained from the distance between the terminal or file server itself and a plurality of GPS satellites or a plurality of portable telephone base stations. In specific embodiments, the communicable range of each terminal and file server is decided, and the communication range is controlled from the position information received from each terminal and file server.

[0059] One aspect of the invention provides a network connection environment only within a limited range by limiting the communicable range and rejecting a network connection from an unexpected terminal appropriately, and an appropriate information transfer can be enabled while preventing a leak of information and preventing access from a disguised user.

[0060] Another aspect of the invention is that in each terminal and file server, the position information of the terminal or file server itself is obtained from the distance between the terminal or file server itself and a plurality of GPS satellites or a plurality of portable telephone base stations, and the information can be applied to security management.

[0061] Yet another aspect is that in the authentication server, the communicable range of each terminal and file server can be determined and the communication range can be controlled from the position information received from each terminal and file server.

[0062] The above-described arrangements of apparatus and methods are merely illustrative of applications of the principles of this invention and many other embodiments and modifications may be made without departing from the spirit and scope of the invention as defined in the claims. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the appended claims along with their full scope of equivalents.